In the Claims:

1.   (Currently Amended) A cryptographic device
comprising:

an input stage receiving an input data block <u>that is X</u>
<u>bits in length</u> and a key data block comprising a plurality of
sub-key data blocks, <u>said input stage adding the X bits of the</u>
<u>input data block with a first sub-key data block to generate a</u>
<u>summed signal that is X bits in length, and then dividing the</u>
<u>summed signal into N</u> ~~and generating a plurality of~~ first signals
~~therefrom~~ that are in parallel<u>, where each first signal is n bits</u>
<u>in length so that n * N = X</u>;

an intermediate stage connected to said input stage and
comprising

a plurality of substitution units operating in
parallel, each substituting data within a respective
first signal, and

a diffuser connected to said plurality of
substitution units for mixing data to generate a
diffused signal, said diffuser comprising at least one
shift register and at least one look-up table
associated therewith; and

an output stage connected to said intermediate stage
for repetitively looping back the diffused signal to said input
stage for combination with a next sub-key data block.

2.   (Original) A cryptographic device according to
Claim 1 wherein the looping back is repeated a predetermined

number of times; and wherein said output stage provides an output signal for the cryptographic device after the repetitively looping back is complete.

3.   (Original) A cryptographic device according to Claim 2 wherein the output signal is further combined with a final sub-key data block.

4.   (Original) A cryptographic device according to Claim 1 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table.

Claim 5 (Cancelled).

6.   (Previously Presented) A cryptographic device according to Claim 1 wherein said at least one shift register comprises a plurality of shift registers and said at least one look-up table comprises a plurality of look-up tables associated therewith.

7.   (Original) A cryptographic device according to Claim 1 wherein said output stage performs a row-shift operation on the diffused output signal before being looped back to said input stage.

8.   (Original) A cryptographic device according to Claim 1 wherein said output stage performs a column-mix operation on the diffused output signal being looped back to said input

3

stage.

9.   (Original) A cryptographic device according to
Claim 1 wherein said output stage comprises a counter for
counting a number of times the diffused output signal is looped
back to said input stage.

10.   (Currently Amended) A communication system
comprising:
a key scheduler providing a key data block comprising a
plurality of sub-key data blocks; and
a cryptographic device connected to said key scheduler
and comprising

an input stage receiving an input data block <u>that</u>
<u>is X bits in length</u> and the key data block, <u>said input</u>
<u>stage adding the X bits of the input data block with a</u>
<u>first sub-key data block to generate a summed signal</u>
<u>that is X bits in length, and then dividing the summed</u>
<u>signal into N</u> ~~and generating a plurality of~~ first
signals ~~therefrom~~ that are in parallel<u>, where each</u>
<u>first signal is n bits in length so that n * N = X</u>;
an intermediate stage connected to said input
stage and comprising
a plurality of substitution units
operating in parallel, each substituting data
within a respective first signal, and
a diffuser connected to said plurality
of substitution units for mixing data to

4

generate a diffused signal, said diffuser

comprising at least one shift register and at

least one look-up table associated therewith,

and

an output stage connected to said intermediate

stage for repetitively looping back the diffused signal

to said input stage for combination with a next sub-key

data block, said output stage providing an output

signal for the cryptographic device after the

repetitively looping back is complete.

11.   (Original) A communication system according to

Claim 10 wherein the output signal is further combined with a

final sub-key data block.

12.   (Original) A communication system according to

Claim 10 wherein each substitution unit performs a non-linear

substitution based upon at least one look-up table.

Claim 13 (Cancelled).

14.   (Previously Presented) A communication system

according to Claim 10 wherein said at least one shift register

comprises a plurality of shift registers and said at least one

look-up table comprises a plurality of look-up tables associated

therewith.

15.   (Original) A communication system according to

Claim 10 wherein said output stage performs a row-shift operation on the diffused output signal before being looped back to said input stage.

16.   (Original) A communication system according to Claim 10 wherein said output stage performs a column-mix operation on the diffused output signal being looped back to said input stage.

17.   (Original) A communication system according to Claim 10 wherein said output stage comprises a counter for counting a number of times the diffused output signal is looped back to said input stage.

18.   (Currently Amended) A method for converting an input data block that is X bits in length and a key data block comprising a plurality of sub-key data blocks into an output signal in a cryptographic device, the method comprising:

~~generating a plurality of first signals that are in parallel based upon the input data block and a key data block comprising a plurality of sub-key data blocks;~~

adding the X bits of the input data block with a first sub-key data block to generate a summed signal that is X bits in length, and then dividing the summed signal into N first signals that are in parallel, where each first signal is n bits in length so that n * N = X;

substituting data within each first signal using a respective substitution unit, with the substitution units

operating in parallel to one another;

mixing data to generate a diffused signal using a diffuser connected to the respective substitution units, the diffuser comprising at least one shift register and at least one look-up table associated therewith; and

repetitively looping back the diffused signal for combination with a next sub-key data block before repeating the substituting and mixing.

19.   (Original) A method according to Claim 18 wherein the looping back is repeated a predetermined number of times; and further comprising providing an output signal for the cryptographic device after the repetitively looping back is complete.

20.   (Original) A method according to Claim 19 further comprising combining the output signal with a final sub-key data block.

21.   (Original) A method according to Claim 18 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table.

Claim 22 (Cancelled).

23.   (Previously Presented) A method according to Claim 18 wherein the at least one shift register comprises a plurality of shift registers and the at least one look-up table comprises a

plurality of look-up tables associated therewith.

24.   (Original) A method according to Claim 18 further comprising performing a row-shift operation on the diffused output signal before being looped back.

25.   (Original) A method according to Claim 18 further comprising performing a column-mix operation on the diffused output signal being looped back.

26.   (Original) A method according to Claim 18 further comprising counting a number of times the diffused output signal is looped back.